A proof of the Corrected Beiter conjecture

Jia Zhao, Xianke Zhang

Abstract

We say that a cyclotomic polynomial $\Phi_n(x)$ has order three if n is the product of three distinct primes, $p < q < r$. Let $A(n)$ be the largest absolute value of a coefficient of $\Phi_n(x)$ and $M(p)$ be the maximum of $A(pqr)$. In 1968, Sister Marion Beiter conjectured that $A(pqr) \leqslant \frac{p+1}{2}$. In 2008, Yves Gallot and Pieter Moree showed that the conjecture is false for every $p \geqslant 11$, and they proposed the Corrected Beiter conjecture: $A(pqr) \leqslant \frac{2}{3}p$. Here we will give a proof of this conjecture.

Key words: Cyclotomic polynomial, Corrected Beiter conjecture
1991 MSC: 11B83, 11C08

1. Introduction

The nth cyclotomic polynomial is the monic polynomial whose roots are the primitive nth roots of unity and are all simple. It is defined by

$$\Phi_n(x) = \prod_{\substack{1 \leqslant a \leqslant n \\ (a,n)=1}} (x - e^{\frac{2\pi i a}{n}}) = \sum_{i=0}^{\phi(n)} c_i x^i.$$

The degree of Φ_n is $\phi(n)$, where ϕ is the Euler totient function. It is known that the coefficients c_i, where $0 \leqslant i \leqslant \phi(n)$, are all integers.

Definition 1.1.

$$A(n) = \max\{|c_i|, 0 \leqslant i \leqslant \phi(n)\}.$$

For $n < 105$, $A(n) = 1$. It was once conjectured that this would hold for all n, however $A(105) = 2$. Note that 105 is the smallest positive integer that is the product of three distinct odd primes. In fact, it is easy to prove that $A(p) = 1$ and $A(pq) = 1$ for distinct primes p, q. Besides, we have the following useful propositions.

Proposition 1.2. *The nonzero coefficients of* $\Phi_{pq}(x)$ *alternate between* $+1$ *and* -1.

Proposition 1.3. *Let* p *be a prime.*
If $p \mid n$*, then* $\Phi_{pn}(x) = \Phi_n(x^p)$*, so* $A(pn) = A(n)$*.*
If $p \nmid n$*, then* $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$*.*
If n *is odd, then* $\Phi_{2n}(x) = \Phi_n(-x)$*, so* $A(2n) = A(n)$*.*

Proof. See [9] for details. □

By the proposition above, it suffices to consider squarefree values of n to determine $A(n)$. For squarefree n, the number of distinct odd prime factors of n is the order of the cyclotomic polynomial Φ_n. Therefore the cyclotomic polynomials of order three are the first non-trivial case with respect to $A(n)$. We also call them ternary cyclotomic polynomials.

Assume $p < q < r$ are odd primes, Bang [2] proved the bound $A(pqr) \leqslant p-1$. This was improved by Beiter [3, 4], who proved that $A(pqr) \leqslant p - \lfloor \frac{p}{4} \rfloor$, and made the following conjecture.

Conjecture 1.4 ((Beiter)). $A(pqr) \leqslant \frac{p+1}{2}$.

Beiter proved her conjecture for $p \leqslant 5$ and also in case either q or $r \equiv \pm 1 \pmod{p}$ [3]. If this conjecture holds, it is the strongest possible result of this form. This is because Möller [10] indicated that for any prime p there are infinitely many pairs of primes $q < r$ such that $A(pqr) \geqslant \frac{p+1}{2}$. Define

$$M(p) = \max\{A(pqr) \mid p < q < r\},$$

where the prime p is fixed, and q and r are arbitrary primes. Now with Möller's result, we can reformulate Beiter's conjecture.

Conjecture 1.5. For $p > 2$, we have $M(p) = \frac{p+1}{2}$.

However, Gallot and Moree [6] showed that Beiter's conjecture is false for every $p \geqslant 11$. Based on extensive numerical computations, they gave many counter-examples and proposed the Corrected Beiter conjecture.

Conjecture 1.6 ((Corrected Beiter conjecture)). We have $M(p) \leqslant \frac{2}{3}p$.

This is the strongest corrected version of Beiter's conjecture because they also proved that for any $\varepsilon > 0$, $\frac{2}{3}p(1-\varepsilon) \leqslant M(p) \leqslant \frac{3}{4}p$ for every sufficiently large prime p. In this paper, we will give a proof of the Corrected Beiter conjecture.

2. Main theorem

First we introduce some notation for the rest of the paper. Let $p < q < r$ be odd primes. Let

$$\Phi_{pqr}(x) = \sum_i c_i x^i,$$

and

$$\Phi_{pq}(x) = \sum_m d_m x^m.$$

For $i < 0$ or $i > \phi(pqr) = (p-1)(q-1)(r-1)$, $m < 0$ or $m > \phi(pq) = (p-1)(q-1)$, we set $c_i = d_m = 0$.

Notation 2.1. $\forall n \in \mathbb{Z}$, let $\overline{n}$ be the unique integer such that $0 \leqslant \overline{n} \leqslant pq - 1$ and $\overline{n} \equiv n \pmod{pq}$.

Definition 2.2. For any $n \in \mathbb{Z}$, define a map

$$\chi_n : \mathbb{Z} \longrightarrow \{0, \pm 1\}$$

by

$$\chi_n(i) = \begin{cases} 1 & \text{if } \overline{n+p+q} \geqslant \overline{i+1} > \overline{n+q} \text{ or} \\ & \overline{i+1} \leqslant \overline{n+p+q} < \overline{n+q} \text{ or} \\ & \overline{n+p+q} < \overline{n+q} < \overline{i+1}, \\ -1 & \text{if } \overline{n+p} \geqslant \overline{i+1} > \overline{n} \text{ or} \\ & \overline{i+1} \leqslant \overline{n+p} < \overline{n} \text{ or} \\ & \overline{n+p} < \overline{n} < \overline{i+1}, \\ 0 & \textit{otherwise.} \end{cases}$$

It is easy to certify that the value of $\chi_n(i)$ only depends on $\overline{n}$ and $\bar{i}$. That means for any $n', i' \in \mathbb{Z}, n' \equiv n \pmod{pq}, i' \equiv i \pmod{pq}$, we have

$$\chi_{n'}(i') = \chi_n(i).$$

With notation as above, now we recall some important results. For the details, we refer the reader to our previous paper [11].

Lemma 2.3. *We have*

$$c_i = \sum_{mr+p+q \geqslant i+1+pq} d_m \chi_{mr}(i).$$

Corollary 2.4. *For any integer i,*

$$\sum_m d_m \chi_{mr}(i) = 0.$$

Corollary 2.5. *We have*

$$A(pqr) \leqslant \max_{i,j\in\mathbb{Z}} \left| \sum_{m\geqslant j} d_m \chi_{mr}(i) \right| .$$

Remark 2.6. If q and r interchange, we will have similar arguments as above.

By corollary 2.3, we know it is sufficient for estimating the upper bound of $A(pqr)$ to consider $\max_{i,j\in\mathbb{Z}} \left| \sum_{m\geqslant j} d_m \chi_{mr}(i) \right|$. Therefore we need to study the coefficients d_m of Φ_{pq}.

Notation 2.7. For any distinct primes p and q, let q_p^* be the unique integer such that $0 < q_p^* < p$ and $qq_p^* \equiv 1 \pmod p$. Let $\overline{q_p}$ be the unique integer such that $0 < \overline{q_p} < p$ and $q \equiv \overline{q_p} \pmod p$.

About the coefficients of Φ_{pq}, Lam and Leung [8] showed

Theorem 2.8 ((T.Y. Lam and K.H. Leung, 1996))**.** *Let $\Phi_{pq}(x) = \sum_m d_m x^m$. For $0 \leqslant m \leqslant \phi(pq)$, we have*

(A) $d_m = 1$ if and only if $m = up + vq$ for some $u \in [0, p_q^* - 1]$ and $v \in [0, q_p^* - 1]$;

(B) $d_m = -1$ if and only if $m + pq = u'p + v'q$ for some $u' \in [p_q^*, q-1]$ and $v' \in [q_p^*, p-1]$;

(C) $d_m = 0$ otherwise.

The numbers of terms of the former two kinds are, respectively, $p_q^* q_p^*$ and $(q - p_q^*)(p - q_p^*)$, with difference 1 since $(p-1)(q-1) = (p_q^* - 1)p + (q_p^* - 1)q$.

About $A(pqr)$, the best known general upper bound to date is due to Bartłomiej Bzdęga [5]. He gave the following important result

Theorem 2.9 ((Bartłomiej Bzdęga, 2008))**.** *Set*

$$\alpha = \min\{q_p^*, r_p^*, p - q_p^*, p - r_p^*\}$$

and $0 < \beta < p$ satisfying $\alpha\beta qr \equiv 1 \pmod p$. Put $\beta^* = \min\{\beta, p - \beta\}$. Then we have

$$A(pqr) \leqslant \min\{2\alpha + \beta^*, p - \beta^*\}.$$

Now we can prove our main theorem.

Theorem 2.10 ((Corrected Beiter conjecture)). *Assume $p < q < r$ are odd primes. Let $\Phi_{pqr}(x) = \sum_i c_i x^i$ and $A(pqr) = \max\{|c_i|, 0 \leqslant i \leqslant \phi(pqr)\}$. Then we have $A(pqr) \leqslant \frac{2}{3}p$.*

Proof. Suppose $A(pqr) > \frac{2}{3}p$, we will show that this is a contradiction. Let us first assume

$$1 \leqslant p - q_p^* \leqslant r_p^* < p - r_p^* \leqslant q_p^* \leqslant p - 1. \tag{2.1}$$

By Remark 1, we can observe that the proof is similar for the other cases. According to Theorem 2.5, it follows $\alpha = p - q_p^*$, $\beta = p - r_p^*$ and $\beta^* = r_p^*$. Since $A(pqr) > \frac{2}{3}p$, so we easily get

$$\beta^* < \frac{1}{3}p. \tag{2.2}$$

By Corollary 2.3, we know there exist a pair of integers i, j such that

$$\left|\sum_{m \geqslant j} d_m \chi_{mr}(i)\right| > \frac{2}{3}p. \tag{2.3}$$

By Theorem 2.4, we can divide the nonzero terms of $\Phi_{pq}(x)$ into p classes depending on the value of v or v'. From the definition of χ_n, we can simply verify that for any given class, there is at most one term such that $\chi_{mr}(i) = 1$. For the case $\chi_{mr} = -1$, we have the similar result.

Since $(up + vq)r + p \equiv (up + (v - r_p^*)q)r + p + q \pmod{pq}$, it follows

$$\chi_{mr}(i) = -1 \Longleftrightarrow \chi_{(m - r_p^* q)r}(i) = 1. \tag{2.4}$$

We claim that

$$\sum_{m \geqslant j} d_m \chi_{mr}(i) < -\frac{2}{3}p. \tag{2.5}$$

By (2.3), we know $\sum_{m \geqslant j} d_m \chi_{mr}(i) > \frac{2}{3}p$ or $\sum_{m \geqslant j} d_m \chi_{mr}(i) < -\frac{2}{3}p$. However the number of the classes of $d_m = -1$ is just $p - q_p^*$, hence

$$\sum_{m \geqslant j, d_m = -1} d_m \chi_{mr}(i) \leqslant \lfloor \frac{1}{3}p \rfloor.$$

If the former holds, then

$$\sum_{m\geqslant j, d_m=1} d_m\chi_{mr}(i) \geqslant \lfloor\frac{1}{3}p\rfloor + 1 \tag{2.6}$$

Thus there must exist $u \in [0, p_q^*-1]$ and $v \in [0, q_p^*-1-\lfloor\frac{1}{3}p\rfloor]$ such that $\chi_{(up+vq)r}(i) = 1$. By (2.4), we have $\chi_{(up+(v+r_p^*)q)r}(i) = -1$ and $v + r_p^* \in [0, q_p^*-1]$. Hence $d_{up+vq}\chi_{(up+vq)r}(i) + d_{up+(v+r_p^*)q}\chi_{(up+(v+r_p^*)q)r}(i) = 0$, their contributions to the left side of (2.6) are zero. This is a contradiction, so we establish our claim.

With the arguments above, now we can give the following definition. For any class v, $v \in [0, q_p^*-1]$, if there exist $u_1, u_2 \in [0, p_q^*-1]$ such that $u_1p+vq \geqslant j > u_2p+vq$, $\chi_{(u_1p+vq)r}(i) = -1$ and $\chi_{(u_2p+vq)r}(i) = 1$, then we say it is a special class. If there exists either u_1 or u_2 satisfying the above conditions, we say it is a plain class. If there exists neither u_1 nor u_2 satisfying the above conditions, we say it is a null class. Similarly for any class v', $v' \in [q_p^*, p-1]$, if there exist $u_1', u_2' \in [p_q^*, q-1]$ such that $u_1'p+v'q-pq \geqslant j > u_2'p+v'q-pq$, $\chi_{(u_1'p+v'q-pq)r}(i) = 1$ and $\chi_{(u_2'p+v'q-pq)r}(i) = -1$, then we say it is a special class. If there exists either u_1' or u_2' satisfying the above conditions, we say it is a plain class. If there exists neither u_1' nor u_2' satisfying the above conditions, we say it is a null class. Let S, P and N denote the sets of the special classes, the plain classes and the null classes respectively.

By Corollary 2.2 and (2.3), we immediately obtain

$$\left|\sum_{m<j} d_m\chi_{mr}(i)\right| > \frac{2}{3}p. \tag{2.7}$$

By (2.3) and (2.7), it is easy to verify that

$$|S| - |N| > \frac{1}{3}p. \tag{2.8}$$

The number of the classes v', $v' \in [q_p^*, p-1]$ is just $p - q_p^*$, so there must exist at least one v, $v \in [0, q_p^*-1]$ such that $v \in S$. Let v_0 be the largest value of $v \in [0, q_p^*-1]$ such that $v \in S$. Next we will consider three cases according to the value of v_0 and derive a contradiction to (2.8) to complete the proof.

Case 1. $q_p^* - r_p^* \leqslant v_0 \leqslant q_p^* - 1$

First we claim that for any class v, $v \in [0, q_p^*-1]$, if $v \in S$, then $v_0 - r_p^* + 1 \leqslant v \leqslant v_0$.

Obviously we only need to show the first inequality. Suppose $0 \leqslant v \leqslant v_0 - r_p^*$ and $v \in S$. By the definition of the special class, we know there exist $u_2, u_3 \in [0, p_q^* - 1]$ such that

$$u_2p + v_0q < j, \chi_{(u_2p+v_0q)r}(i) = 1$$

and

$$u_3p + vq \geqslant j, \chi_{(u_3p+vq)r}(i) = -1.$$

This yields

$$u_3p + vq > u_2p + v_0q,$$

hence

$$(u_3 - u_2)p > (v_0 - v)q \geqslant r_p^*q.$$

On the other hand,

$$(u_3 - u_2)p \leqslant (p_q^* - 1)p = (p - q_p^*)q - p + 1 \leqslant r_p^*q - p + 1.$$

The equality holds because $(p-1)(q-1) = (p_q^* - 1)p + (q_p^* - 1)q$. Therefore we derive a contradiction and prove our claim.

Now we consider the classes v', $v' \in [q_p^*, p-1]$. Since $v_0 \in S$, $v_1' = v_0 + r_p^* \notin S$. If not, then there exists $u_2' \in [p_q^*, q-1]$ such that $\chi_{(u_2'p+(v_0+r_p^*)q-pq)r}(i) = -1$. By (2.4), we get $\chi_{((u_2'-q)p+v_0q)r}(i) = 1$. On the other hand, there exists $u_2 \in [0, p_q^* - 1]$ such that $\chi_{(u_2p+v_0q)r}(i) = 1$. By the definition of χ_n, we have $q \mid (u_2' - u_2)$, however it is impossible.

Suppose $q_p^* \leqslant v_2' \leqslant v_0 + r_p^* - 1$ and $v_2' \in S$. Similarly we know $v_2' - r_p^* \in [v_0 - r_p^* + 1, v_0]$, but $v_2' - r_p^* \notin S$. Moreover, if $v_2' - r_p^* \in N$, then the contributions of these two classes to the left side of (2.8) are zero, thus we can ignore them. If $v_2' - r_p^* \in P$, then we say the class v_2' is a valid special class. Let S_0 denote the set of the valid special classes.

Suppose $v_0 + r_p^* + 1 \leqslant v_3' \leqslant p-1$ and $v_3' \in S_0$. We claim that $2v_0 + r_p^* - v_3' \in [v_0 - r_p^* + 1, v_0]$ and $2v_0 + r_p^* - v_3' \notin S$.

Since $v_0 \in S$, there exist $u_1, u_2 \in [0, p_q^* - 1]$ such that $u_1p + v_0q \geqslant j > u_2p + v_0q$, $\chi_{(u_1p+v_0q)r}(i) = -1$ and $\chi_{(u_2p+v_0q)r}(i) = 1$. This implies that

$$\overline{(u_1p + v_0q)r + p + \overline{q_p}} = \overline{(u_2p + v_0q)r + p + q} \qquad (2.9)$$

or

$$\overline{(u_1p + v_0q)r + p - (p - \overline{q_p})} = \overline{(u_2p + v_0q)r + p + q}. \qquad (2.10)$$

Since $v_3' \in S$, there exist $u_3', u_4' \in [p_q^*, q-1]$ such that $u_3'p + v_3'q - pq \geqslant j > u_4'p + v_3'q - pq$, $\chi_{(u_3'p+v_3'q-pq)r}(i) = 1$ and $\chi_{(u_4'p+v_3'q-pq)r}(i) = -1$. This implies that

$$\overline{(u_3'p + v_3'q - pq)r + p + q - \overline{q_p}} = \overline{(u_4'p + v_3'q - pq)r + p} \tag{2.11}$$

or

$$\overline{(u_3'p + v_3'q - pq)r + p + q + (p - \overline{q_p})} = \overline{(u_4'p + v_3'q - pq)r + p}. \tag{2.12}$$

If (2.9) and (2.11) hold simultaneously, then we get

$$\overline{(u_1 + u_3')pr} = \overline{(u_2 + u_4')pr}.$$

Hence

$$q \mid (u_1 + u_3' - u_2 - u_4').$$

This is impossible. Similarly (2.10) and (2.12) can not hold simultaneously either, so without loss of generality we assume (2.10) and (2.11) are correct. By (2.4), we have $\chi_{(u_4'p+v_3'q-pq-r_p^*q)r}(i) = 1$. Because $v_3' \in S_0$, we know there exists $u_5 \in [0, p_q^*-1]$ such that $u_5p + (v_3' - r_p^*)q \geqslant j$ and $\chi_{(u_5p+(v_3'-r_p^*)q)r}(i) = -1$. Hence

$$\overline{(u_5p + (v_3' - r_p^*)q)r + p + \overline{q_p}} = \overline{((u_4' - q)p + (v_3' - r_p^*)q)r + p + q} \tag{2.13}$$

or

$$\overline{(u_5p + (v_3' - r_p^*)q)r + p - (p - \overline{q_p})} = \overline{((u_4' - q)p + (v_3' - r_p^*)q)r + p + q}. \tag{2.14}$$

If (2.14) holds, by (2.10) we get

$$\overline{(u_5 - u_1)pr} = \overline{(u_4' - q - u_2)pr}.$$

Hence

$$q \mid (u_5 + u_2 - u_1 - u_4'). \tag{2.15}$$

On the other hand, by

$$u_5p + (v_3' - r_p^*)q \geqslant j > u_4'p + v_3'q - pq$$

we have

$$0 > (u_5 - u_4')p > (r_p^* - p)q.$$

Note that

$$0 > (u_2 - u_1)p \geqslant -(p_q^* - 1)p = -(p - q_p^*)q + p - 1 \geqslant -r_p^* q + p - 1,$$

so we can get

$$0 > (u_5 + u_2 - u_1 - u_4')p > -pq + p - 1.$$

This contradicts (2.15) and establishes the validity of (2.13).

Now if $2v_0 + r_p^* - v_3' \in S$, then there exist $u_7, u_8 \in [0, p_q^* - 1]$ such that $u_7 p + (2v_0 + r_p^* - v_3')q \geqslant j > u_8 p + (2v_0 + r_p^* - v_3')q$, $\chi_{(u_7p+(2v_0+r_p^*-v_3')q)r}(i) = -1$ and $\chi_{(u_8p+(2v_0+r_p^*-v_3')q)r}(i) = 1$. By (2.10), we have

$$\overline{(u_7 p + (2v_0 + r_p^* - v_3')q)r + p - (p - \overline{q_p})} = \overline{(u_8 p + (2v_0 + r_p^* - v_3')q)r + p + q}. \tag{2.16}$$

We recall that $\overline{q_p} \leqslant \frac{p-1}{3}$ and refer the reader to the proof of the main result in [11]. Combining (2.10), (2.13) and (2.16) yields

$$\begin{aligned}&\overline{((u_4' - q)p + (v_3' - r_p^*)q)r + p + q} + \overline{(u_8 p + (2v_0 + r_p^* - v_3')q)r + p + q}\\ =&\overline{2((u_2 p + v_0 q)r + p + q)}\end{aligned}$$

Hence

$$q \mid u_4' + u_8 - 2u_2. \tag{2.17}$$

Moreover, we have $u_7 > u_2$ because $u_7 p + (2v_0 + r_p^* - v_3')q \geqslant j > u_2 p + v_0 q$ and $2v_0 + r_p^* - v_3' < v_0$. It follows

$$u_4' - u_2 > u_1 - u_2 = u_7 - u_8 > u_2 - u_8.$$

The equality is easily obtained by (2.10) and (2.16). Therefore

$$u_4' + u_8 - 2u_2 = q,$$

and

$$2(q - u_4') = 2(u_8 - 2u_2) \leqslant 2(p_q^* - 1). \tag{2.18}$$

On the other hand, by (2.11) and (2.13) we get

$$q \mid u_3' + u_5 - 2u_4'.$$

In view of the ranges of u_3', u_4' and u_5, we certainly have

$$u_3' + u_5 - 2u_4' = 0,$$

and

$$2(q-u_4') > q+u_3'-2u_4' = q-u_5 \geqslant q-p_q^*+1. \tag{2.19}$$

By (2.18) and (2.19), we get

$$p_q^*-1 > \frac{1}{3}q.$$

Since $q_p^* > \frac{2}{3}p$, it is a contradiction, so we prove our claim.

Finally, we need to show that if $2(v_0+r_p^*)-v_3' \in [q_p^*, v_0+r_p^*-1]$, then $v_3' \in S_0$ and $2(v_0+r_p^*)-v_3' \in S_0$ can not hold simultaneously. Otherwise, there exist $u_5', u_6' \in [p_q^*, q-1]$ such that $u_5'p+(2(v_0+r_p^*)-v_3')q-pq \geqslant j > u_6'p+(2(v_0+r_p^*)-v_3')q-pq$, $\chi_{(u_5'p+(2(v_0+r_p^*)-v_3')q-pq)r}(i) = 1$ and $\chi_{(u_6'p+(2(v_0+r_p^*)-v_3')q-pq)r}(i) = -1$. By (2.4), we have

$$\chi_{(u_6'p+(2v_0+r_p^*-v_3')q-pq)r}(i) = 1.$$

Because $2(v_0+r_p^*)-v_3' \in S_0$, we know there exists $u_9 \in [0, p_q^*-1]$ such that $u_9p+(2v_0+r_p^*-v_3')q \geqslant j$ and

$$\chi_{(u_9p+(2v_0+r_p^*-v_3')q)r}(i) = -1.$$

Hence it follows

$$\overline{(u_9p+(2v_0+r_p^*-v_3')q)r+p+\overline{q_p}} = \overline{((u_6'-q)p+(2v_0+r_p^*-v_3')q)r+p+q}. \tag{2.20}$$

Combining (2.10), (2.13) and (2.20) yields

$$\begin{aligned}&\overline{((u_4'-q)p+(v_3'-r_p^*)q)r+p+q}+\overline{(u_9p+(2v_0+r_p^*-v_3')q)r+p}\\=&\overline{(u_1p+v_0q)r+p}+\overline{(u_2p+v_0q)r+p+q}\end{aligned}$$

Hence

$$q \mid u_4'+u_9-u_1-u_2. \tag{2.21}$$

Moreover $u_9 > u_2$ and $u_4' > u_1$, so

$$u_4'+u_9-u_1-u_2 = q,$$

and

$$2(q-u_4') = 2(u_9-u_1-u_2) \leqslant 2(p_q^*-1). \tag{2.22}$$

By (2.19) and (2.22), we get a contradiction and establish the claim. Now combining our arguments above shows that

$$|S|-|N| \leqslant r_p^* < \frac{1}{3}p.$$

This contradicts (2.8) and completes the proof. In the remaining two cases, the methods which will be used are similar to the present case, so we will introduce our ideas and omit the straightforward details.

Case 2. $r_p^* \leqslant v_0 \leqslant q_p^* - r_p^* - 1$

First we know for any class v, $v \in [0, q_p^* - 1]$, if $v \in S$, then $v_0 - r_p^* + 1 \leqslant v \leqslant v_0$.

Suppose $v_0 - r_p^* + 1 \leqslant v_1 \leqslant 2v_0 + r_p^* - q_p^*$ and $v_1 \in S$. Then $2v_0 - v_1 + r_p^* \geqslant q_p^*$ and $2v_0 - v_1 + r_p^* \notin S_0$.

For any class v_2, $2v_0 + r_p^* - q_p^* + 1 \leqslant v_2 \leqslant v_0 - 1$, we consider the class $2v_0 - v_2$. Obviously, $2v_0 - v_2 \notin S$. If $2v_0 - v_2 \in P$, then the class $2v_0 - v_2 + r_p^* \in N$ or $2v_0 - v_2 - r_p^* \in N$. Combining the arguments above, we get

$$|S| - |N| \leqslant \max\{r_p^*, p - q_p^* + 1\}.$$

By (2.8), it follows $|S| - |N| = p - q_p^* + 1$, so

$$p - q_p^* = r_p^* = \frac{p-1}{3}, v_0 = r_p^*. \tag{2.23}$$

If $1 \leqslant v_3 \leqslant v_0 - 1$ and $v_3 \in S$, then $v_3 - r_p^* + p \in [q_p^* + 1, p - 1]$ and $v_3 - r_p^* + p \notin S$. Thus we have

$$|S| = p - q_p^* + 1, |N| = 0. \tag{2.24}$$

We claim that for any class v_4, $v_0 \leqslant v_4 \leqslant q_p^* - 1$, there must exist $u_1 \in [0, p_q^* - 1]$ such that $u_1 p + v_4 q \geqslant j$ and $\chi_{(u_1 p + v_4 q)r}(i) = -1$. Obviously it holds for the classes v_0 and $q_p^* - 1$. If it is not correct for a class $v_4 \in [v_0 + 1, q_p^* - 2]$, then for the class $v_4 - r_p^*$, by (2.4), there does not exist $u_4 \in [0, p_q^* - 1]$ such that $u_4 p + (v_4 - r_p^*)q < j$ and $\chi_{(u_4 p + (v_4 - r_p^*)q)r}(i) = 1$. Therefore $v_4 - r_p^* \notin S$, $v_4 - r_p^* \in P$. Then there exists $u_3 \in [0, p_q^* - 1]$ such that $u_3 p + (v_4 - r_p^*)q \geqslant j$ and $\chi_{(u_3 p + (v_4 - r_p^*)q)r}(i) = -1$. It is not difficult to obtain that $v_4 - 2r_p^* + p \notin S$. This implies $|S| \leqslant p - q_p^*$. It contradicts (2.24) and establishes the claim.

By (2.24), we know $q_p^* \in S_0$. Similar to the arguments in case 1, we can get $2v_0 + r_p^* - q_p^* = r_p^* - 1 \notin S$. Thus $p - 1 \in S$. Moreover, by the previous claim, we know $p - 1 \in S_0$. In fact, for any $v_1' \in [q_p^* + 1, p - 2]$, we have $v_1' \in S_0$. Otherwise, $v_1' \in P$, then $v_1' + r_p^* - p \in S$ and $2v_0 + r_p^* - v_1' \notin S$. This implies the class $2v_0 - v_1' + p \in S$. However, $v_1' + r_p^* - p \in S$ and $2v_0 - v_1' + p \in S$ can not hold simultaneously.

With the arguments above, we know there exist $u_1', u_2' \in [p_q^*, q-1]$ such that $\chi_{(u_1'p+(p-1)q-pq)r}(i) = 1$ and $\chi_{(u_2'p+(p-1)q-pq)r}(i) = -1$. By (2.11), we get

$$\overline{(u_1'p + (p-1)q - pq)r + p + q - \overline{q_p}} = \overline{(u_2'p + (p-1)q - pq)r + p}. \quad (2.25)$$

By (2.4), we have $\chi_{((u_2'-q)p+2r_p^*q)r}(i) = 1$ and $\chi_{(u_1'p+(r_p^*-1)q)r}(i) = -1$. By the claim above, we know there exist $u_5, u_8 \in [0, p_q^*-1]$ such that $\chi_{(u_5p+2r_p^*q)r}(i) = -1$ and $\chi_{(u_8p+(r_p^*-1)q)r}(i) = 1$. By (2.13), we get

$$\overline{(u_5p + 2r_p^*q)r + p + \overline{q_p}} = \overline{((u_2' - q)p + 2r_p^*q)r + p + q}, \quad (2.26)$$

and

$$\overline{(u_1'p + (r_p^* - 1)q)r + p + \overline{q_p}} = \overline{(u_8p + (r_p^* - 1)q)r + p + q}. \quad (2.27)$$

Combining (2.25), (2.26) and (2.27) yields

$$\overline{(u_5p + 2r_p^*q)r + p + 3\overline{q_p}} = \overline{(u_8p + (r_p^* - 1)q)r + p + q}. \quad (2.28)$$

We also have $\chi_{(u_8p+(2r_p^*-1)q)r}(i) = -1$. It follows

$$\overline{(u_8p + (r_p^* - 1)q)r + p + q} = \overline{(u_8p + (2r_p^* - 1)q)r + p},$$

hence we have

$$\overline{(u_5p + 2r_p^*q)r + p + 3\overline{q_p}} = \overline{(u_8p + (2r_p^* - 1)q)r + p}. \quad (2.29)$$

Since $v_0 = r_p^* \in S$, there exists $u_9 \in [0, p_q^* - 1]$ such that $\chi_{(u_9p+r_p^*q)r}(i) = -1$. Thus by (2.29), we have

$$\overline{(u_9p + r_p^*q)r + p} = \overline{(u_5p + 2r_p^*q)r + p + 3r_p^*\overline{q_p}}. \quad (2.30)$$

On the other hand, $\chi_{(u_5p+r_p^*q)r}(i) = 1$. By (2.10), we have

$$\overline{(u_9p + r_p^*q)r + p - (p - \overline{q_p})} = \overline{(u_5p + r_p^*q)r + p + q}. \quad (2.31)$$

(2.30) and (2.31) yields

$$\overline{(u_9p + r_p^*q)r + p} = \overline{(u_9p + r_p^*q)r + p - (p - \overline{q_p}) + 3r_p^*\overline{q_p}} \quad (2.32)$$

Note that $p = 3r_p^* + 1$. Hence (2.32) means that $\overline{q_p} = 1$, but it is impossible. Therefore we get a contradiction and complete the proof of the present case.

Case 3. $0 \leqslant v_0 \leqslant r_p^* - 1$

Suppose $v \in [0, v_0]$ and $v \in S$, then we have $v - r_p^* + p \leqslant p - 1$. If $v - r_p^* + p \geqslant q_p^*$, then $v - r_p^* + p \notin S$. Therefore we have

$$|S| \leqslant r_p^* < \frac{1}{3}p.$$

This contradicts (2.8) and completes the proof of the theorem. □

References

[1] G. Bachman, On the coefficients of ternary cyclotomic polynomials, J. Number Theory 100 (2003) 104-116.

[2] A.S. Bang, Om Lingingen $\Phi_n(x) = 0$, Tidsskr. Math. 6 (1895) 6–12.

[3] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}, Amer. Math. Monthly 75 (1968) 370–372.

[4] M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}, II, Duke Math. J. 38 (1971) 591–594.

[5] B. Bzdęga, Bounds on ternary cyclotomic coefficients, arXiv:0812.4024, preprint.

[6] Y. Gallot and P. Moree, Ternary cyclotomic polynomials having a large coefficient, J. Reine Angew. Math. 632(2009), 105-125.

[7] N. Kaplan, Flat cyclotomic polynomials of order three, J. Number Theory 127 (2007) 118–126.

[8] T.Y. Lam, K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, Amer. Math. Monthly 103 (1996) 562-564.

[9] H.W. Lenstra, Vanishing sums of roots of unity, in:Proceedings, Bicentennial Congress Wiskundig Genootschap, Vrije Univ., Amsterdam, 1978, PartII, 1979, pp. 249-268.

[10] H. Möller, Über die Koeffizienten des n-ten Kreisteilungspolynoms, Math. Z. 119 (1971) 33–40.

[11] Jia Zhao, Xianke Zhang, On the coefficients of the cyclotomic polynomials of order three, arXiv:0910.1982, preprint.

Department of Mathematical Sciences, Tsinghua University,
Beijing 100084, China
E-mail: zhaojia@mails.tsinghua.edu.cn; xzhang@math.tsinghua.edu.cn